# Algebraic Number Theory
# MATH 512

## Solutions to Assignment 2

**1.** Let $H_\alpha = \mathrm{Gal}(M/\mathbb{Q}(\alpha))$, which contains $H$. Let $B$ be a set of representatives for $(G/H_\alpha)_{\text{left}}$ and $C$ a set of representatives for $(H_\alpha/H)_{\text{left}}$. Then $\{\tau\rho \mid \tau \in B \text{ and } \rho \in C\}$ is a set of representatives for $(G/H)_{\text{left}}$. Since $g_\alpha(x)$ is independent of the choice of set of representatives for $(G/H)_{\text{left}}$, we see that

$$\begin{aligned} g_\alpha(x) &= \prod_{\substack{\tau \in B \\ \rho \in C}} (x - \tau\rho(\alpha)) \\ &= \prod_{\tau \in B} (x - \tau(\alpha))^{[L:\mathbb{Q}(\alpha)]}. \end{aligned}$$

We claim that $G$ acts on $\{\tau(\alpha) \mid \tau \in B\}$. Indeed, if $\sigma \in G$ then $\sigma\tau = \tau'\sigma'$ for some $\tau' \in B$ and some $\sigma' \in H_\alpha$, so $\sigma\tau(\alpha) = \tau'\sigma'(\alpha) = \tau'(\alpha)$. Therefore, letting $f_\alpha(x) = \prod_{\tau \in B}(x - \tau(\alpha))$, we see that $G$ fixes $f_\alpha(x)$. Hence $f_\alpha(x) \in \mathbb{Q}[x]$. Since $\alpha$ is a root of $f_\alpha(x)$, and since $f_\alpha(x)$ has degree $|G : H_\alpha| = [\mathbb{Q}(\alpha) : \mathbb{Q}]$, $f_\alpha(x)$ is the minimal polynomial for $\alpha$ over $\mathbb{Q}$.

Now, if $\alpha \in \mathcal{O}_L$ then by Proposition 4, $f_\alpha(x) \in \mathbb{Z}[x]$ and therefore $g_\alpha(x) = f_\alpha(x)^{[L:\mathbb{Q}(\alpha)]} \in \mathbb{Z}[x]$. Conversely, if $g_\alpha(x) \in \mathbb{Z}[x]$, then $\alpha$ is a root of a monic polynomial with integer coefficients and therefore lies in $\mathcal{O}_L$.

**2.** Let $\overline{f}(x)$ be the reduction mod $\mathfrak{p}$ of the minimal polynomial of $\alpha$ over $K$. Firstly, if $\mathfrak{p}$ splits completely then there are $n = [L : K]$ primes above $\mathfrak{p}$, each of ramification index and residue degree 1 over $\mathfrak{p}$. Therefore $\overline{f}(x)$ splits into $n$ linear factors over $k(\mathfrak{p})$, and so in particular has a root in $k(\mathfrak{p})$, i.e. $f(x)$ has a root mod $\mathfrak{p}$.

Conversely, suppose that $\overline{f}(x)$ has a root, so that $\overline{f}(x)$ has a monic linear factor $\overline{P}(x)$. Let $\mathfrak{P}$ be the prime of $B$ corresponding to this linear factor. Observe that $f(\mathfrak{P}|\mathfrak{p}) = \deg(\overline{P}(x)) = 1$. Also, by assumption $\mathfrak{p}$ is unramified in $B$ and so $e(\mathfrak{P}|\mathfrak{p}) = 1$. Finally, since $L/K$ is Galois, $e(\mathfrak{P}'|\mathfrak{p}) = e(\mathfrak{P}|\mathfrak{p}) = 1$ and $f(\mathfrak{P}'|\mathfrak{p}) = f(\mathfrak{P}|\mathfrak{p}) = 1$ for all $\mathfrak{P}'|\mathfrak{p}$, and so $\mathfrak{p}$ splits completely in $B$.

**3.** (a) Since $a \mapsto a^2$ defines a ring homomorphism in characteristic 2, the reduction of $x^4 - x^2 + 1$ mod 2 is equal to $(x^2 - x + 1)^2$. We can see that $x^2 - x + 1$ is irreducible over $\mathbb{F}_2$ by checking for roots, but we know it has to be anyway since 2 is ramified in $L$. Reducing $x^4 - x^2 + 1$ mod 3, we see that it factorizes as $(x^2 + 1)^2$. The polynomial $x^2 + 1$ is irreducible over $\mathbb{F}_3$, but again, we knew it had to be because 3 ramifies in $L$.

(b) This is just question 2 applied to the extension $L/\mathbb{Q}$.

(c) By assumption, $12|p - 1$, and so there is $\overline{a} \in \mathbb{F}_p^\times$ whose order is exactly

12. Therefore in $\mathbb{F}_p$,

$$\begin{aligned} 0 &= \overline{a}^{12} - 1 \\ &= (\overline{a}-1)(\overline{a}+1)(\overline{a}^2+\overline{a}+1)(\overline{a}^2+1)(\overline{a}^2-\overline{a}+1)(\overline{a}^4-\overline{a}^2+1). \quad (1) \end{aligned}$$

None of the first five factors in (1) can be zero since, in each case, there is a divisor $m < 12$ of 12 such that the factor divides $\overline{a}^m - 1$. That leaves $\overline{a}^4 - \overline{a}^2 + 1 = 0$, i.e. $p | a^4 - a^2 + 1$.

(d) (i) Since $x^4 - x^2 + 1$ divides $x^{12} - 1$, the assumption on $a$ implies that $a^{12} - 1 \equiv 0 \bmod p$, so $a$ has order dividing 12.

(ii) Observe that for each divisor $m < 12$ of 12, the element $\overline{a}^m - 1$ is a product of a subset of the first five factors in (1). Therefore, by assuming $a$ has order strictly less than 12, we must have $h(a) \equiv 0 \bmod p$ where $h(x)$ is one of the first five polynomials in the right-hand side of equation (1) of the question sheet. Let $f(x) = x^4 - x^2 + 1$, and write $x^{12} - 1 = f(x)h(x)g(x)$. Since $p$ divides both $f(a)$ and $h(a)$, $a^{12} - 1 \equiv 0 \bmod p^2$. Further, $f(a+p) \equiv f(a) \equiv 0 \bmod p$, and similarly for $h(a+p)$, so

$$\begin{aligned} (a+p)^{12} - 1 &= f(a+p)h(a+p)g(a+p) \\ &\equiv 0 \bmod p^2. \end{aligned}$$

(iii) We have

$$\begin{aligned} 0 &\equiv (a+p)^{12} - 1 \bmod p^2 \\ &\equiv a^{12} + 12a^{11}p - 1 \bmod p^2 \\ &\equiv 12a^{11}p \bmod p^2, \end{aligned}$$

showing that $p^2 | 12a^{11}p$, i.e. $p | 12a^{11}$, a contradiction.

(iv) The order of $a$ mod $p$ necessarily divides $p-1$. In this case, we therefore have $12 | p-1$, i.e. $p \equiv 1 \bmod 12$.

**4.** Any element of $\mathrm{Gal}(M/K)$ which fixes $\mathfrak{P}$ must, when restricted to $L$, fix $\mathfrak{q}$. Thus $E|_L \subseteq D$, showing $L^D \subseteq M^E$ and hence $L^D \subseteq L \cap M^E$. In fact, $L^D = L \cap M^E$: If $\mathfrak{p}'$ is the prime of $L^D$ below $\mathfrak{P}$ and $\mathfrak{p}''$ is the prime of $L \cap M^E$ below $\mathfrak{P}$, then $e(\mathfrak{p}''|\mathfrak{p}') = f(\mathfrak{p}''|\mathfrak{p}') = 1$ because both these fields lie in the extension $M^E/K$. On the other, since $L \cap M^E$ is an intermediate field in the extenion $L/L^D$, $\mathfrak{p}''$ is the unique prime of $L \cap M^E$ above $\mathfrak{p}'$, so $L \cap M^E = L^D$.

Now let $\mathfrak{P}'$ be the prime of $LM^E$ below $\mathfrak{P}$. Since $LM^E$ is an intermediate field in the extension $M/M^E$, $\mathfrak{P}$ is the unique prime of $M$ above $\mathfrak{P}'$. On the other hand, by our assumption on $e(\mathfrak{P}|\mathfrak{q})$ and $f(\mathfrak{P}|\mathfrak{q})$, we have $e(\mathfrak{P}|\mathfrak{P}') = f(\mathfrak{P}|\mathfrak{P}') = 1$, showing that $M = LM^E$. Galois theory completes the proof.

**5.** Let $\mathfrak{p}$ be a prime of $K$ and $\mathfrak{P}$ a prime of $L$ above $\mathfrak{p}$. If $\mathfrak{p}$ is non-split, then $G_{\mathfrak{P}} = G$, and so $I_{\mathfrak{P}}$ is normal in $G$ with $G/I_{\mathfrak{P}} \simeq \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$, which is cyclic. However, if $\mathfrak{p}$ is further unramified, then $I_{\mathfrak{P}}$ is trivial and so $G$ is cyclic. Thus if $G$ is not cyclic, then any non-split prime must be ramified. Since there are only ever finitely many ramified primes, there can only be finitely many non-split primes in this case.